(12) UK Patent Application (19) GB (11) 2 294 853 (13) A

(43) Date of A Publication 08.05.1996

(21) Application No 9522786.4

(22) Date of Filing 07.11.1995

(30) Priority Data
(31) 945222 (32) 07.11.1994 (33) FI

(71) Applicant(s)
Nokia Telecommunications OY

(Incorporated in Finland)

Mäkkylän Puistotie 1, SF-02600 Espoo, Finland

(72) Inventor(s)
Juha Heikkilä
Harri Hurme

(74) Agent and/or Address for Service
Frank B Dehn & Co
Imperial House, 15-19 Kingsway, LONDON,
WC2B 6UZ, United Kingdom

(51) INT CL^6
H04L 25/03 , H04J 14/08 , H04K 1/00 , H04L 9/18

(52) UK CL (Edition O)
H4P PPEB

(56) Documents Cited
GB 2258590 A EP 0652661 A2 EP 0308150 A1
WO 95/01019 A1 US 4972479 A

(58) Field of Search
UK CL (Edition O) H4B BK12C , H4P PDCSL PDCSP PDCSX PPEB , H4R RCT
INT CL^6 H04B 10/12 , H04J 14/08 , H04K 1/00 , H04L 9/00 9/18 12/22 25/03
Online: WPI, INSPEC

(54) **Subscriber-specific scrambling and descrambling in a subscriber network**

(57) To provide a simple and flexible equipment for data scrambling in a subscriber network based on a point-to-multipoint system, the scrambling sequences of the subscribers currently corresponding to the time slots of the transmission frame of a signal to be transmitted to subscriber terminals are stored in the central unit of the network, in RAM 61, and the scrambling sequence of a subscriber corresponding to the current time slot of the transmission frame is read to the scrambling means 67 located in the central unit to scramble the subscriber data by the subscriber's own scrambling sequence. The invention also relates to descrambling implemented in similar manner, using descrambling means 65.

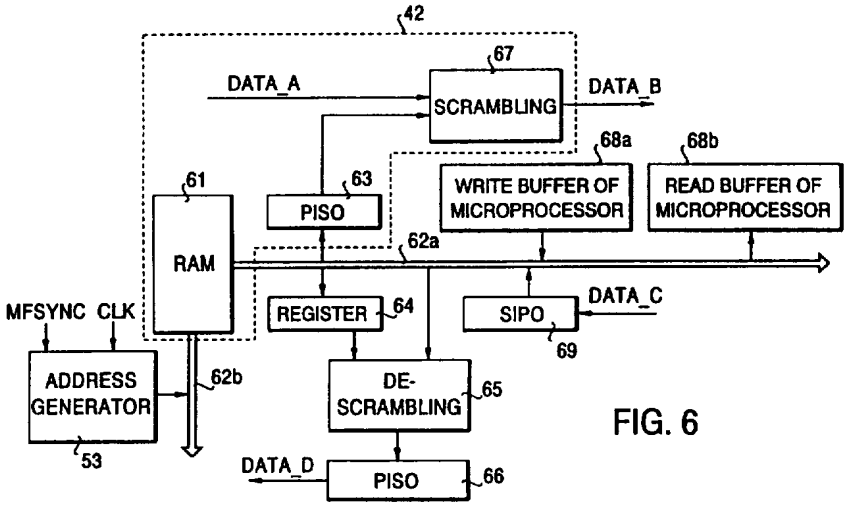

FIG. 6

GB 2 294 853 A

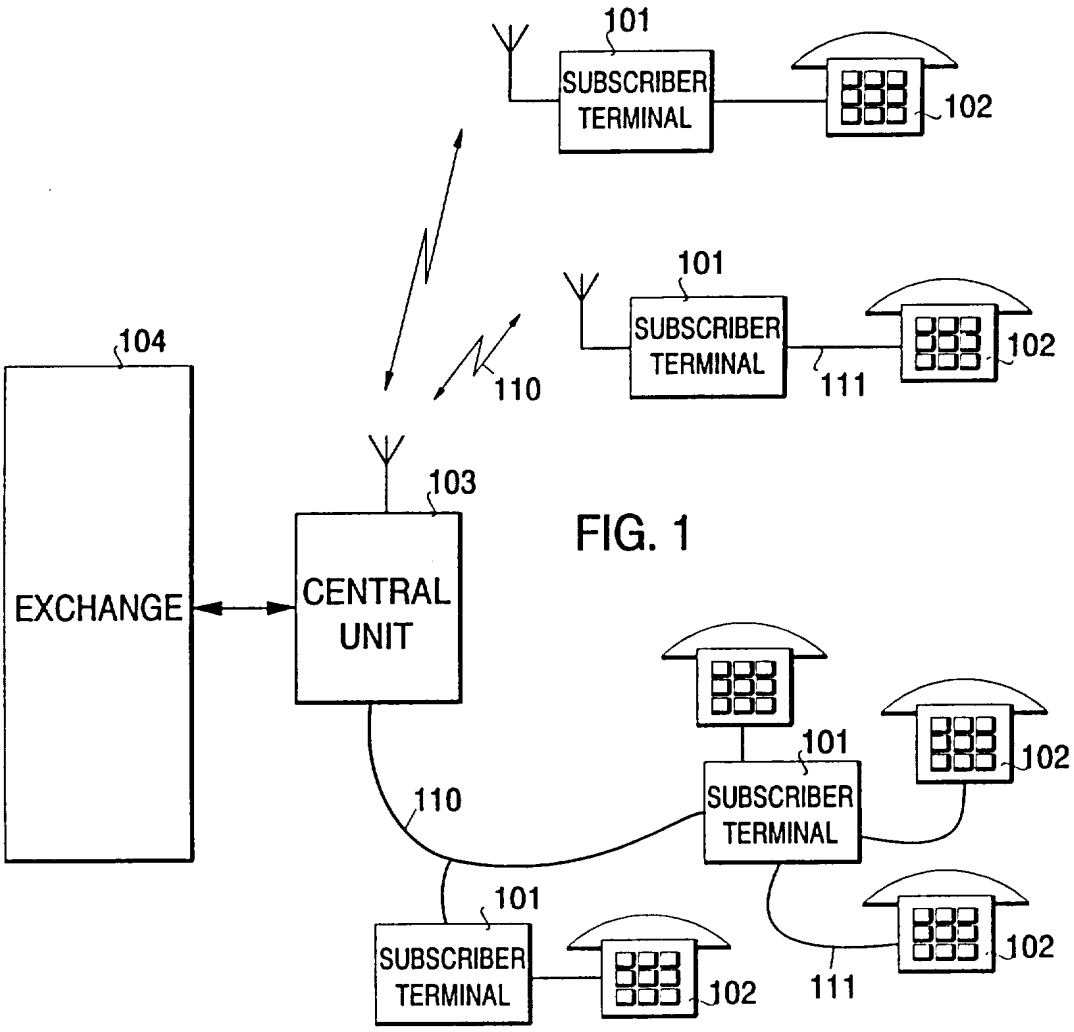
101
SUBSCRIBER TERMINAL
102
101
SUBSCRIBER TERMINAL
102
111
104
110
103
EXCHANGE
CENTRAL UNIT
101
SUBSCRIBER TERMINAL
102
110
101
SUBSCRIBER TERMINAL
102
111
102

FIG. 1

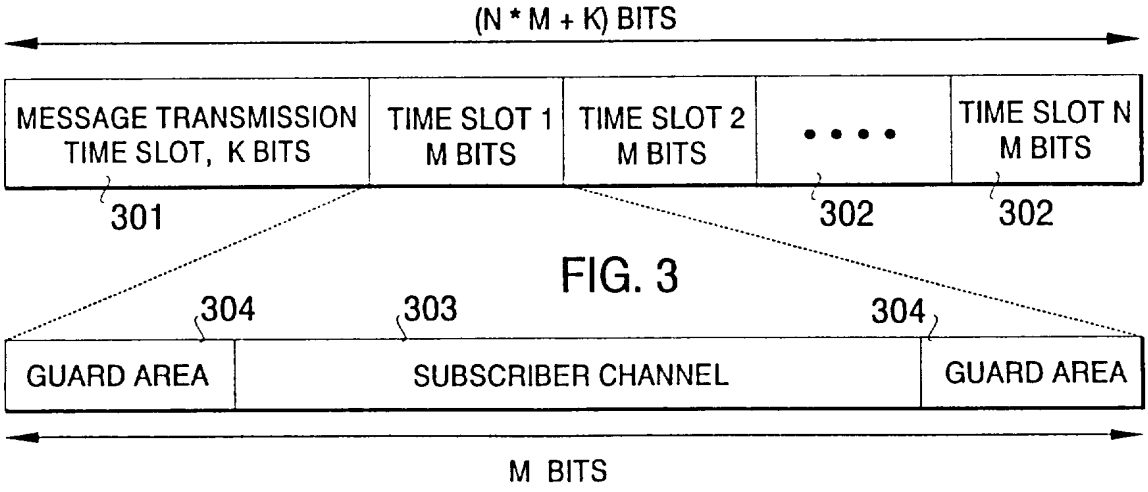
(N * M + K) BITS
MESSAGE TRANSMISSION TIME SLOT, K BITS
TIME SLOT 1 M BITS
TIME SLOT 2 M BITS
• • • •
TIME SLOT N M BITS
301
302
302
304
303
304
GUARD AREA
SUBSCRIBER CHANNEL
GUARD AREA
M BITS

FIG. 3

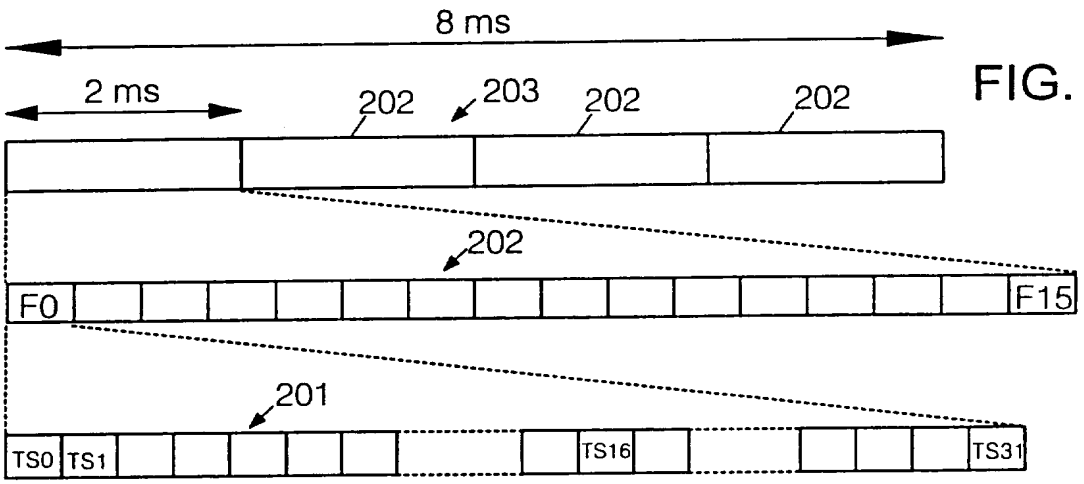

FIG. 2a

FRAME NO.	BIT CONTENTS OF TIME SLOTS TS0							
	b1	b2	b3	b4	b5	b6	b7	b8
F0	C	KL	KL	KL	KL	KL	KL	KL
F1	(0)	1	X	S	S	S	S	S
F2	C	KL	KL	KL	KL	KL	KL	KL
F3	(0)	1	X	S	S	S	S	S
F4	C	KL	KL	KL	KL	KL	KL	KL
F5	(1)	1	X	S	S	S	S	S
F6	C	KL	KL	KL	KL	KL	KL	KL
F7	(0)	1	X	S	S	S	S	S
F8	C	KL	KL	KL	KL	KL	KL	KL
F9	(1)	1	X	S	S	S	S	S
F10	C	KL	KL	KL	KL	KL	KL	KL
F11	(1)	1	X	S	S	S	S	S
F12	C	KL	KL	KL	KL	KL	KL	KL
F13	SF	1	X	S	S	S	S	S
F14	C	KL	KL	KL	KL	KL	KL	KL
F15	SF	1	X	S	S	S	S	S

FIG. 2b

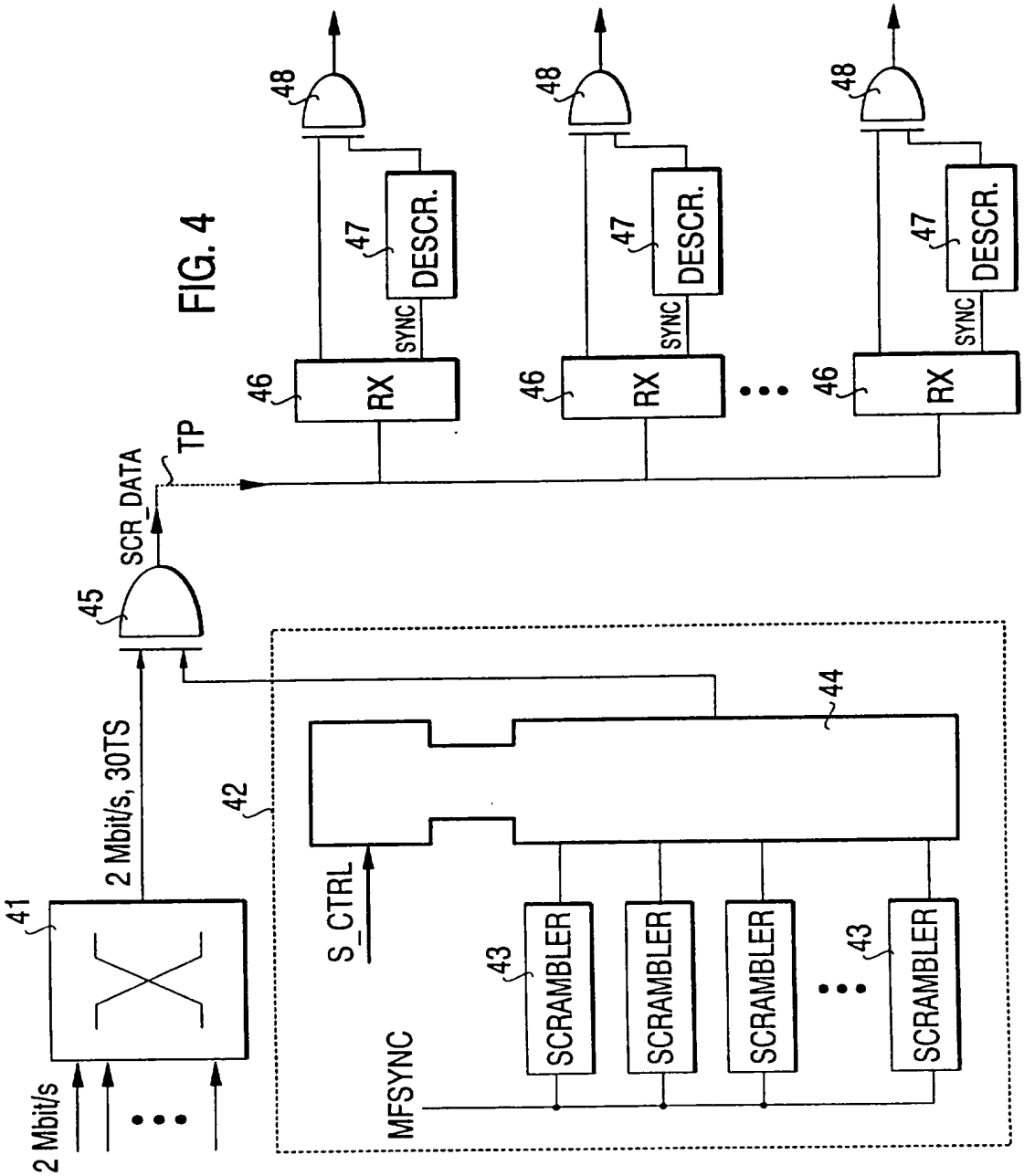
2 Mbit/s
41
2 Mbit/s, 30TS
42
S_CTRL
MFSYNC
43
SCRAMBLER
44
45
SCR_DATA
TP
46
RX
SYNC
47
DESCR.
48

FIG. 4

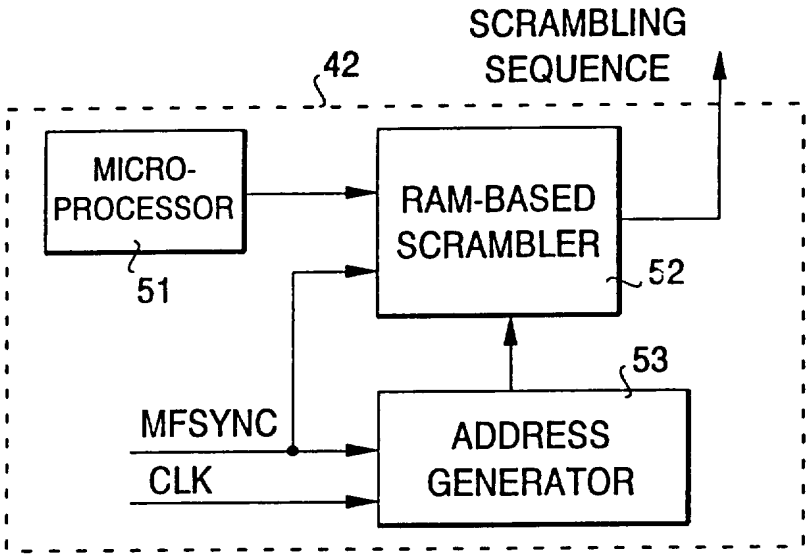
SCRAMBLING
SEQUENCE
42
MICRO-
PROCESSOR
51
RAM-BASED
SCRAMBLER
52
53
MFSYNC
CLK
ADDRESS
GENERATOR

FIG. 5

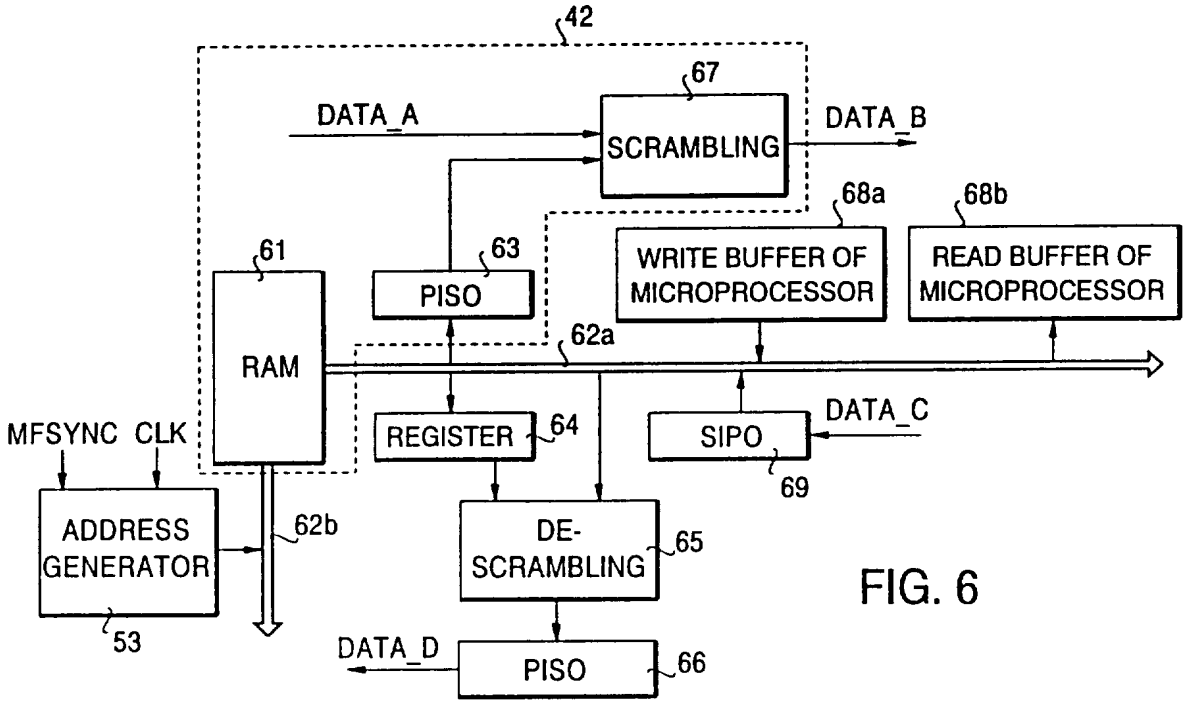
42
67
DATA_A
SCRAMBLING
DATA_B
68a
68b
61
63
WRITE BUFFER OF
MICROPROCESSOR
READ BUFFER OF
MICROPROCESSOR
PISO
RAM
62a
MFSYNC CLK
REGISTER
64
SIPO
DATA_C
69
ADDRESS
GENERATOR
62b
DE-
SCRAMBLING
65
53
DATA_D
PISO
66

FIG. 6

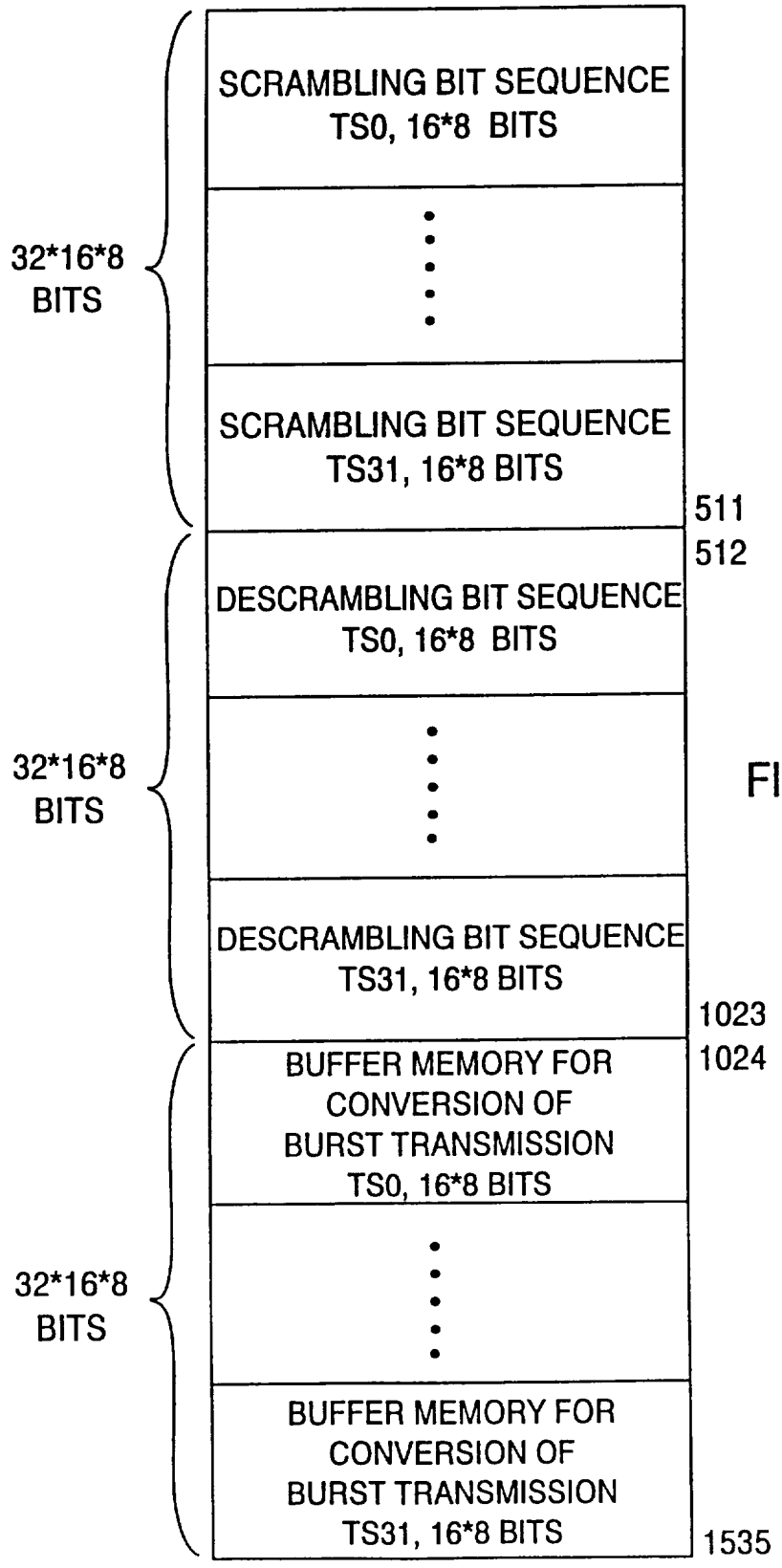
SCRAMBLING BIT SEQUENCE TS0, 16*8 BITS
SCRAMBLING BIT SEQUENCE TS31, 16*8 BITS
511
512
DESCRAMBLING BIT SEQUENCE TS0, 16*8 BITS
DESCRAMBLING BIT SEQUENCE TS31, 16*8 BITS
1023
1024
BUFFER MEMORY FOR CONVERSION OF BURST TRANSMISSION TS0, 16*8 BITS
BUFFER MEMORY FOR CONVERSION OF BURST TRANSMISSION TS31, 16*8 BITS
1535
32*16*8 BITS
32*16*8 BITS
32*16*8 BITS

FIG. 7

Method and equipment for implementing subscriber-specific scrambling and descrambling in a subscriber network

The invention relates to a method described in the preamble of attached claim 1 for implementing subscriber-specific scrambling in a point-to-multipoint system based on time divisional data transmission. The invention also relates to a method for implementing subscriber-specific descrambling in such a point-to-multipoint system, and equipment implementing the scrambling and/or descrambling in such a point-to-multipoint system.

The solution of the invention is especially well-suited for use in cable television and telephone networks, Passive Optical Networks (PON), and in connection with a wireless local loop. Because of the point-to-multipoint character of the connection, it must be possible in these networks to prevent a third party from listening to a call and to prevent a call from being switched to a wrong time slot due to a malfunction in a subscriber set. This can be effected by encrypting every channel by a subscriber-specific encryption key. Effective encryption, however, is a rather complicated and expensive process, and too massive for normal subscriber connections. The forwarded data is sufficiently protected if a data scrambler associated with a normal modem is modified such that a different scrambling sequence is provided by the scrambler for each subscriber.

In known scramblers, a scrambling sequence is typically formed by a feedback shift register. The circuitry allows production of a pseudorandom bit sequence, which is added to payload data in a transmitter by modulo-2-addition. Descrambling is

performed with a similar equipment in a receiver by adding the same pseudorandom bit sequence to a received data stream by modulo-2-addition.

A known method like this is useful in a point-to-point connection, where all the bits of a data stream pass through the same scrambler and descrambler. Subscriber-specific scrambling of a connection can be implemented by loading into the shift register a subscriber-specific seed number, on the basis of which a sequence is formed.

If, however, each time slot of a time divisional signal is to be scrambled by a subscriber-specific sequence, a different scrambler is needed for each time slot. A 30 time slot system, for example, must then have 30 parallel scramblers, only one of which is used at a time. If the system is a concentrated system (number of subscribers exceeds number of time slots), a different scrambling sequence is needed for each subscriber, which may be difficult to implement e.g. in a system comprising 120 subscribers. Because of this, time-slot-specific data scrambling has hardly been used at all in known solutions.

Another problem with known solutions is that scramblers are inflexible in respect of the sequence used. If a sequence is to be modified, the scrambler circuitry has to be changed. Even though it is possible to change the circuitry e.g. by means of controllable feedback branches, it should be noted that the number of shift register implementations providing a sensible scrambling sequence is limited. Thereby the only flexible way of modifying a sequence is to change the starting point of the sequence by means of the seed number loaded into the shift register.

In known solutions, data scrambling and

encryption are two quite separate functions. This guarantees, on the one hand, sufficient randomness between the symbols transmitted, as required by data transmission, and, on the other hand, good protection for the information transmitted. Equipments like these, however, are rather complicated and expensive.

The object of the present invention is to provide a solution without the above drawbacks. This is achieved with the methods of the invention, which are characterized by what is disclosed in the characterizing parts of attached claims 1 (scrambling) and 5 (descrambling). The equipments of the invention, in turn, are characterized by what is disclosed in the characterizing parts of attached claims 6 and 8.

The idea of the invention is to perform data scrambling and descrambling time-slot-specifically in a central unit of a point-to-multipoint system by a scrambler/descrambler that is based on a (RAM) memory located in the central unit rather than on permanent circuitry, sequences being stored in said memory time-slot-specifically. When in each time slot, scrambling sequence data of a corresponding subscriber is read out from the memory, a time divisional signal is produced from which the receiving subscribers are able to pick only the data of their own time slot in decrypted form.

The solution of the invention provides a simple and flexible equipment for scrambling and descrambling data in a subscriber network based on a point-to-multipoint system. A further advantage of the inventive solution is that the memory-based scrambler/descrambler can also be used for performing other functions, such as encryption, conversion of the frame structure, and cross-connection.

The solution of the invention does not make the scramblers of a point-to-multipoint system any more

complicated than e.g. the conventional scramblers of a point-to-point connection are.

The solution of the invention also allows more advanced encryption, since a scrambling sequence can be easily modified even in the middle of an on-going call.

In the following the invention and its preferred embodiments will be described in greater detail with reference to the examples illustrated by the attached drawings, in which

fig. 1 shows a subscriber network forming a typical environment for applying the invention,

fig. 2a shows a more detailed view of a frame structure used on downlink connections in the network of fig. 1,

fig. 2b shows bits transferred in time slots TS0 of successive frames of one multiframe on downlink connections,

fig. 3 shows a frame structure used on uplink connections in a network of fig. 1,

fig. 4 shows a known straightforward way of implementing scrambling and descrambling in a system of fig. 1, the system optionally being a concentrated system,

fig. 5 shows a scrambling unit implemented on the principle described in the invention, the scrambling unit replacing the scrambling unit of the exchange end in the equipment of fig. 4,

fig. 6 shows an equipment of the invention implementing scrambling and descrambling, and

fig. 7 shows one possible memory map of the RAM memory shown in fig. 6.

Fig. 1 shows a subscriber network implemented by means of time-division multipoint access. The network comprises several subscriber terminals 101, to each of which is connected a telephone or some other

such terminal equipment 102 of one or more subscribers, and a central unit 103 common to all the subscriber terminals. The central unit is an equipment establishing a point-to-multipoint connection and connecting the subscribers to an exchange 104 of a Public Switched Telephone Network, PSTN. As an interface is used one of the standardized digital interface methods, such as V2 or V5.1 or V5.2, the latter also making concentration possible (number of subscribers exceeds number of time slots).

The subscriber terminals 101 may be devices positioned at a subscriber, or a subscriber terminal may be a subscriber multiplexer known per se, e.g. a Nokia ACM2 subscriber multiplexer, supplemented e.g. with a modem establishing an RF connection, and framing circuits needed for forming a transmission frame to be transmitted in the uplink direction.

A transmission channel 110 between a subscriber terminal and a central unit may be a radio channel, e.g. a coaxial cable of a cable television network, or even a Passive Optical Network (PON). Combinations of these can also be used such that in different directions of transmission, the physical transmission media forming the transmission path are different. This is advantageous e.g. in situations where a fixed unidirectional distribution network already exists, whereby communication in the uplink direction can be implemented e.g. over a radio path.

A copper cable 111 extending from a subscriber terminal to a subscriber set 102 is in practice very short, only about 100 m even at its longest.

For a more detailed description of networks of the type described above, reference is made to Finnish Patent Application No. 932,818. The publication contains a more detailed description of the structure

of e.g. the central unit 103 and the subscriber terminal 101.

A downlink connection, i.e. a connection from a central unit to a subscriber terminal, can be implemented in a network of the type described above by modifying the standard 2048 kbit/s frame structure as little as possible but yet in such a way that from the multiplexing system known per se in the frame structure of which separate signalling bits are allocated to each subscriber one changes over to the use of message-based signalling. The modifications are directed to the structure of time slot 0 (TS0), and time slot 16 (TS16) is freed for other than signalling use. Figs. 2a and 2b show a downlink frame structure: fig. 2a shows the actual frame structure and fig. 2b shows signalling to be transmitted in time slot 0 (TS0). A frame of a 2048 kbit/s basic multiplexing system known per se is indicated by 201, the frame being divided into 32 time slots TS0 to TS31, time slots TS1 to TS15 and TS17 to TS31 forming speech channels in the known manner. In the system, sixteen successive frames F0 to F15 form a multiframe 202 of 2 ms in length. The multiframes of 16 frames each can, in turn, form a superframe 203 comprising e.g. four multiframes and thus being 8 ms in length.

A message transmission channel is added to time slot 0 (TS0), the channel consisting of the free bits of the odd frames, as shown in fig. 2b. In time slot 0, the bits indicated by S are signalling message bits; the bits indicated by KL are frame alignment bits; the bits indicated by C are CRC4 bits, by which the quality of the connection is monitored; the bits indicated by SF indicate the number of the multiframe; and the bits indicated by X are stuffing bits of no significance. Bits b1 of the odd frames, circled in

fig. 2b, form a multiframe alignment word in accordance with the CCITT recommendations. The subsequent bits (b2), which are set as 1, indicate that the frame concerned lacks a frame alignment word.

From the signalling bits are formed messages of 40 bits in length (5 bits per frame, 8 frames per multiframe). This is not relevant to the present invention, however, and so reference is made to the above-mentioned FI Pat. Appln. 932,818.

In a network of fig. 1, an uplink connection (i.e. connection from subscriber terminals to a central unit) is preferably implemented by using the frame structure shown in fig. 3. The frame comprises one long time slot 301 for message transmission and several shorter time slots 302 (i.e. typically K>>M) reserved for subscriber communication (speech or data transmission). Each time slot reserved for transmission of information comprises an actual subscriber channel 303 with a guard area 304 of a few bits in length at its both ends. The advantages achieved with a frame structure like this in a network of fig. 1 are described in greater detail in the above-mentioned FI Pat. Appln. 932,818.

The message transmission time slot 301 is used by one subscriber terminal (which may contain more than one subscriber) at a time. A burst sent in a message transmission time slot thus comprises the identifier of the transmitting subscriber terminal. If there is a collision between two subscriber terminals, re-transmission times, which indicate after how many frames re-transmission will be performed, are allotted. In the signalling, e.g. the Slotted Aloha protocol known per se can be used. (The protocol is described in greater detail e.g. in Tanenbaum, A.S.: *Computer Networks*, Englewood Cliffs, 1989, Prentice Hall, Inc.).

In implementing the equipment, it is preferable to select the uplink bit rate such that it is the same as the downlink bit rate, that is e.g. 2048 kbit/s. This makes it simpler to generate e.g. the clock signals needed. With e.g. the following selections:

- number of data transmission time slots: N=54,
- length of data transmission time slots: M=72 bits, and
- length of message transmission time slot: K=208 bits,

an uplink frame comprises a total of 4096 bits, whereby the frame duration is (at a bit rate of 2048 kbit/s) 2 ms, which corresponds to the time needed for transmitting a downlink multiframe.

In the present invention, subscriber-specific scrambling and descrambling are implemented in a time-divisional point-to-multipoint system that was exemplified above. Fig. 4 shows a conventional, straightforward solution for implementing data scrambling and descrambling in a subscriber network having a basic structure according to fig. 1. A subscriber-specific scrambling sequence is formed in a scrambling unit 42, whose output is connected to a first input of an exclusive OR gate 45. To a second input of the exclusive OR gate is applied a signal coming from a cross-connection unit 41, the signal here being a 2 Mbit/s signal that contains 30 speech channels (30 TS). The system is here a concentrated system, whereby it may comprise e.g. 120 subscribers, each of which has his own data scrambler 43. To the data scramblers is applied a multiframe synchronization signal MFSYNC for synchronizing the data scramblers, and the output of each data scrambler is connected to

a selector 44, whose output forms the output of a scrambler unit. The control signals S_CTRL of the selector are used for selecting the output of a scrambler for the output of the selector such that the time slot of a subscriber corresponding to said scrambler is at that particular moment connected to the second input of the exclusive OR gate. In this way, the data of each subscriber is scrambled by a subscriber-specific scrambling sequence at the exclusive OR gate, which outputs a scrambled data stream SCR_DATA. This data stream is transmitted over a transmission path TP (e.g. radio path) to receiving subscriber terminals, which are 120 in all. Each subscriber terminal comprises a receiver unit 46, which forms a scrambled data stream that is supplied to the first input of the exclusive OR gate 48, and a frame or multiframe synchronization signal SYNC that is supplied to a descrambler 47. The synchronization signal is used for synchronizing the descrambler, which forms a subscriber-specific descrambling sequence that is supplied to the second input of the exclusive OR gate 48. Every subscriber is thereby able to descramble his own data only, and is unable to receive data addressed to the other subscribers. The gate 48 outputs the original, unscrambled data stream.

According to the basic idea of the present invention, the scrambling unit 42 is replaced with an equipment shown in fig. 5, the equipment comprising a scrambling block 52 based on a RAM memory, a microprocessor 51 writing the data in the RAM memory and controlling the functions of the equipment, and an address generator unit 53 that allocates turns to those who need the RAM memory. The address generator thus determines e.g. which scrambling sequence stored in the RAM memory is used for generating the output signal of

the scrambling block, or when the microprocessor 51 can read out from the RAM memory or write in it, e.g. modify the sequences stored in the memory. Since the address generator receives a multiframe synchronization signal MFSYNC and a bit clock CLK, it always knows the time slot that is being transmitted or received.

Fig. 6 shows in greater detail the equipment of the invention located in the central unit of a point-to-multipoint system and used not only for data scrambling and descrambling but also for buffering and framing. The solution of figs. 1 to 3, in which the uplink and downlink frequencies are as described, serves here as an example. It must be noted, however, that such frame structures are not necessary for the invention but that the frame structure may vary in many ways.

The equipment comprises a RAM memory block 61 and circuits connected to a data bus 62a or address bus 62b of said block, and scrambling and descrambling gates 67 and 65. In the RAM 61, a different memory area is reserved for the scrambling and descrambling sequences of each time slot. At the beginning of a connection, the sequences of a subscriber operating in the time slot are stored in the RAM. The address generator 53 comprises, in practice, a counter unit and a selector (not shown) arranged to be controlled by the counter unit. The counters of the counter unit count in sync with the downlink and uplink bit rate. The selector always selects the address currently indicated by the counter unit for the address bus 62b of the RAM. The counter unit also provides the read and write commands concerning the RAM, i.e. it informs the circuits connected to the data bus of the RAM block, such as the conversion circuits, registers, and read and write buffers of the microprocessor, when to read

out the information located on the data bus of the RAM block or to write the information from the memory to the data bus. The read and write commands are decoded directly from the readings given by the counter unit in a manner known per se. The above-described control logic operates at a clock frequency that is higher than that of the bit clock, so several read and write turns are available for one information bit processed.

The microprocessor 51 (only the read and write buffers 68b and 68a of the microprocessor are shown in fig. 6) can write in the RAM via a write buffer 68a in the same way as in its own memory. The RAM in its entirety is part of the memory space of the processor, but the memory is also accessible to other elements than the processor.

In this example, the downlink (toward the subscriber) data stream DATA_A (with the exception of the above-described modification of time slot 0) is a standard 2 Mbit/s signal, which is applied to the first input of the scrambling gate 67. The scrambling gate 67 may be e.g. an exclusive OR gate, in the same way as described in fig. 4. A byte of a time-slot-specific scrambling sequence is read out from the RAM block 61 through a parallel/series conversion circuit 63 to the second input of the scrambling gate 67. This function is controlled by the counter unit of the address generator, the counter unit forming the address corresponding to said frame and time slot by means of counters stepping in sync with the downlink frame structure, and commanding the conversion circuit 63 to read out the data located on the data bus of the RAM block, the data consisting of a byte of the scrambling sequence corresponding to the time slot concerned. In the scrambling gate 67, the data bits and scrambling sequence bits are added e.g. by modulo-2-arithmetic,

whereby the scrambling gate outputs a scrambled data stream DATA_B to be forwarded to a subscriber terminal. The downlink bit stream does thus not pass via the RAM memory, but only the bit sequences (i.e. scrambling sequences) read out from the memory are added to the stream.

Descrambling is performed using the same RAM block 61. The burst uplink data stream DATA_C is first converted to a parallel form in the series/parallel conversion circuit 69 as required by the bus, whereafter the data is stored in the memory 61. This must be done, since in this example the transmissions are bursts and therefore differ from the normal 2 Mbit/s frame structure. Bursts coming from different subscribers are stored in the memory, in time-slot-specific memory areas (shown in fig. 7). The storing address for the address bus 62b is obtained from a counter of the counter unit that steps in sync with the bit rate of the uplink frame. The counter unit also gives a write command to the conversion circuit 69. The uplink bit stream stored in the memory is read out from the memory in the order of the normal 2 Mbit/s frame structure, using the time slot and frame synchronization pulses obtained from the downlink frame structure. The actual conversion of the frame structure on an uplink connection occurs as data stored in the memory is read from the address given by the counter unit connected to the address bus.

The data that has been read is descrambled in a descrambling unit 65, which is here of parallel form and may thus consist e.g. of parallel exclusive OR gates in a number (8) corresponding to the length of the byte. Since the memory is a 1-gate RAM, a register 64 is needed for storing either a descrambling sequence or an actual data byte until the other one has been

read out from the memory. Unscrambled data is supplied from the output of the descrambling unit 65 to a parallel/series conversion circuit 66, which outputs a standard 2 Mbit/s signal transmitted in the uplink direction.

Fig. 6 also shows a write buffer 68a and a read buffer 68b of the microprocessor 51, by which the microprocessor can use the RAM memory. When the processor initializes a connection to a subscriber, it writes a subscriber-specific scrambling sequence to a memory block corresponding to the time slot used by the subscriber. The sequence may be one multiframe in length (16 bytes), but longer sequences can also be used. Since the bit sequence (scrambling sequence) performing the scrambling is specific for the subscriber, speech encryption can also be performed by selecting different bit sequences for different subscribers. If the scrambling sequence is only one multiframe in length (16*8 bits) and remains unchanged throughout the connection, the encryption is not very good, but it can be improved by changing the sequence during the connection or by using a bit sequence that is several multiframes in length, since it is thus possible to eliminate e.g. 2 ms cycles in the scrambling sequences used.

Fig. 7 shows one possible memory map of the RAM. The first 512 bytes (addresses 0 to 511) comprise the scrambling sequences of time slots TS0 to TS31. The sequences are here of the same length as a multiframe (16 bytes). The next 512 bytes (addresses 512 to 1023) comprise the descrambling sequences of time slots TS0 to TS31. Memory addresses 1024 to 1535, in turn, function as buffer memory locations, by which data transmitted in the uplink direction is converted from burst form to the form of a standard 2 Mbit/s frame.

The above equipment is able to perform scrambling time-slot-specifically by a bit sequence selected by the user. Since the bit sequence can be selected freely, it is possible to use sequences that are as simple as possible to form in a subscriber terminal. Further, scrambling need not be performed on all time slots, since e.g. a sequence of zeros can be written in the time-slot-specific memory area, whereby said time slot is not, in a way, processed.

The data stream stored in the RAM can also be cross-connected in association with the frame structure conversion. This, however, requires that the cross-connection data should be stored in the RAM memory and taken into account as an address is formed.

At the subscriber terminal end, scrambling/descrambling can be performed by a subscriber-terminal-specific scrambler/descrambler known per se (in the same way as described above in connection with the descrambler in fig. 4).

Although the invention has been described above with reference to examples illustrated by the attached drawings, it is to be understood that the invention is not limited thereto but can be modified within the inventive idea presented above and in the attached claims. For example, descrambling can be performed in the central unit even before the frame structure is converted (and so the transmission frame of the signal mentioned in the attached claims transmitted from subscriber terminals to the telephone network must be understood to cover a frame structure used between subscriber terminals and the central unit and between the central unit and the telephone network). In principle, it is also possible to use the solution of the invention in one direction of the connection only. Also, the memory may, in principle, be

any memory that can be re-written and re-read (if it is sensible in view of the other characteristics of the memory). In practice, the implementation will also be different in respect of e.g. the conversion circuits needed, if a parallel RAM memory according to the above example is not used. Further, the network may be changed in ways that are not bound by the idea of the invention: e.g. the subscriber set and subscriber terminal can, in principle, be integrated into one and the same casing. In this respect, the separate subscriber sets and terminals must be understood in a broader sense.

Claims

1. A method of implementing subscriber-specific scrambling in a subscriber network comprising

- several subscriber sets,
- several subscriber terminals, whereby at least one subscriber set is connected to one subscriber terminal by a transmission connection, and
- a central unit common to several subscriber terminals, the unit connecting the subscriber sets to a public switched telephone network,

in which subscriber network, data transmission between the several subscriber terminals and the central unit is implemented on a time division basis in successive transmission frames via a common transmission path, and in which method

- subscriber-specific scrambling sequences are formed in the central unit, and by each scrambling sequence, the data of the corresponding subscriber is scrambled in scrambling means, characterized in that the scrambling sequences of the subscribers currently corresponding to the time slots of the transmission frame of a signal to be transmitted to subscriber terminals are stored in the central unit of the network, and that scrambling sequence data of a subscriber corresponding to the current time slot of the transmission frame are read to the scrambling means located in the central unit to scramble the subscriber data by the subscriber's own scrambling sequence.

2. A method according to claim 1, characterised in that the scrambling sequence is always initialized at the beginning of a connection.

3. A method according to claim 1, characterised in that the length of the scrambling sequence corresponds to the length of a multiframe.

4. An arrangement according to claim 2,

characterised in that a new sequence will be stored for the subscriber when the connection is active.

5. A method of implementing subscriber-specific descrambling in a subscriber network comprising

- several subscriber sets,
- several subscriber terminals, whereby at least one subscriber set is connected to one subscriber terminal by a transmission connection, and
- a central unit common to several subscriber terminals, the unit connecting the subscriber sets to a public switched telephone network,

in which subscriber network, data transmission between the several subscriber terminals and the central unit is implemented on a time division basis in successive transmission frames via a common transmission path, and in which method

- subscriber-specific descrambling sequences are formed in the central unit, and by each descrambling sequence, the data of the corresponding subscriber is descrambled in descrambling means, characterised in that the descrambling sequences of the subscribers currently corresponding to the time slots of the transmission frame of a signal to be transmitted from the subscriber terminals to the telephone network are stored in the central unit of the network, and that descrambling sequence data of a subscriber corresponding to the current time slot of the transmission frame are read to the descrambling means located in the central unit to descramble the subscriber data by the subscriber's own descrambling sequence.

6. Equipment for implementing subscriber-specific scrambling in a subscriber network comprising

- several subscriber sets,
- several subscriber terminals, whereby at least one subscriber set is connected to one subscriber terminal by a transmission connection, and

- a central unit common to several subscriber terminals, the unit connecting the subscriber sets to a public switched telephone network,

in which subscriber network, data transmission between the several subscriber terminals and the central unit is implemented on a time division basis in successive transmission frames via a common transmission path, the equipment comprising, in the central unit of the network,

- means for forming subscriber-specific scrambling sequences, and

- scrambling means for scrambling subscriber data by a corresponding scrambling sequence, characterized in that the central unit further comprises a memory in which are stored the scrambling sequences of the subscribers corresponding to the time slots of the transmission frame, and means for forwarding the scrambling sequence data of a subscriber corresponding to the current time slot from the memory to the scrambling means to scramble said subscriber data by the subscriber's own scrambling sequence.

7. Equipment according to claim 6, characterized in that the memory is a RAM memory.

8. Equipment for implementing subscriber-specific descrambling in a subscriber network comprising

- several subscriber sets,

- several subscriber terminals, whereby at least one subscriber set is connected to one subscriber terminal by a transmission connection, and

- a central unit common to several subscriber terminals, the unit connecting the subscriber sets to a public switched telephone network,

in which subscriber network, data transmission between the several subscriber terminals and the central unit is implemented on a time division basis in successive transmission frames via a common

transmission path, the equipment comprising, in the central unit of the network,

- means for forming subscriber-specific descrambling sequences, and

- descrambling means for descrambling subscriber data by a corresponding descrambling sequence, characterized in that the central unit further comprises a memory in which are stored the descrambling sequences of the subscribers corresponding to the time slots of the transmission frame, and means for forwarding the descrambling sequence data of a subscriber corresponding to the current time slot from the memory to the descrambling means to descramble said subscriber data by the subscriber's own descrambling sequence.

9. Equipment according to claim 8, characterized in that the memory is a RAM memory.

10. A method of implementing subscriber-specific scrambling in a subscriber network, substantially as hereinbefore described with reference to the accompanying drawings.

11. A method of implementing subscriber-specific descrambling in a subscriber network, substantially as hereinbefore described with reference to the accompanying drawings.

12. Equipment for implementing subscriber-specific scrambling in a subscriber network, substantially as hereinbefore described with reference to the accompanying drawings.

13. Equipment for implementing subscriber-specific descrambling in a subscriber network, substantially as hereinbefore described with reference to the accompanying drawings.

The Patent Office

-20-

Application No: GB 9522786.4
Claims searched: 1-13

Examiner: Keith Williams
Date of search: 31 January 1996

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.O): H4B(BK12C); H4P(PDCSL, PDCSP, PDCSX, PPEB); H4R(RCT)

Int Cl (Ed.6): H04B 10/12; H04J 14/08; H04K 1/00; H04L 9/00, 9/18, 12/22, 25/03

Other: online WPI, INSPEC

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
A	GB 2258590 A	Mitsubishi Denki - see abstract (equivalent to US 5239581)	1,5,6,8
X,P	EP 0652661 A2	A T & T, 10 May 1995 - see column 7, lines 17-55 (equivalent to US 5473696)	1,5,6,8
X	EP 0308150 A1	British Telecom. - see column 3, line 44 to column 4, line 40 (equivalent to US 5144669)	1,5,6,8
A,P	WO 95/01019 A1	Nokia Telecoms. - see whole spec.	
A	US 4972479	Tobias et al. - see abstract (equivalent to WO 91/12679)	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

PUB-NO: GB002294853A
DOCUMENT-IDENTIFIER: GB 2294853 A

TITLE: Subscriber-specific scrambling and descrambling in a subscriber network

PUBN-DATE: May 8, 1996

INVENTOR-INFORMATION:

NAME	COUNTRY
HEIKKILAE, JUHA	N/A
HURME, HARRI	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
NOKIA TELECOMMUNICATIONS OY	FI

APPL-NO: GB09522786
APPL-DATE: November 7, 1995

PRIORITY-DATA: FI00945222A (November 7, 1994)

INT-CL (IPC): H04L025/03 , H04J014/08 , H04K001/00 , H04L009/18

EUR-CL (EPC): H04L009/18 , H04L025/03

ABSTRACT:

CHG DATE=19970802 STATUS=O> To provide a simple and flexible equipment for data scrambling in a subscriber network based on a point-to-multipoint system, the scrambling sequences of the subscribers currently corresponding to the time slots of the transmission frame of a signal to be transmitted to subscriber terminals are stored in the central unit of the network, in RAM 61, and the scrambling sequence of a subscriber corresponding to the current time slot of the transmission frame is read to the scrambling means 67 located in the central unit to scramble the subscriber data by the subscriber's own scrambling sequence. The invention also relates to descrambling implemented in similar manner, using descrambling means 65.